NANOG Presentation

14-JUN-2023

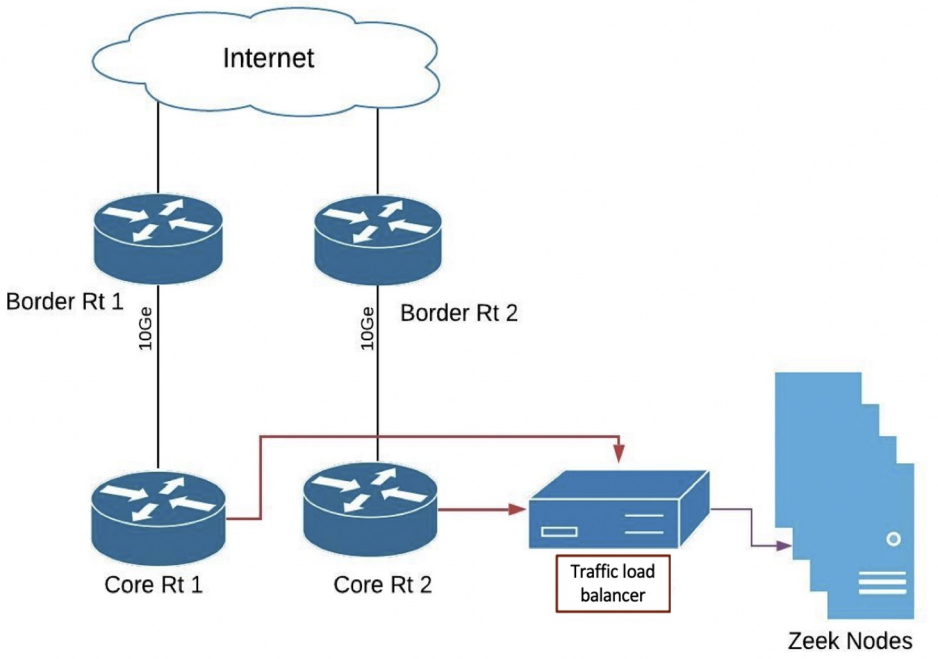
“Off-label” use of DNS

Fatema Bannat Wala
Security Engineer
Berkeley Lab - ESnet
fatemabw@lbl.gov

NANOG™

Network traffic profile (UDel)

- 10 Gbps network links
- Average ~5Gbps network traffic
- Peak ~8Gbps
- 4 Zeek sensors, each getting 25% of total traffic
- Each sensor getting ~300,000pps



Research Problem

- Our research statement of trying to detect well known services that are using DNS for unconventional purposes (“off-label” use) could be summarized in the detailed analysis of two classification techniques:

- *Classification technique 1* : **Hosts that never utilize DNS resolutions**
  - DNS vs TCP connections from the hosts - we analyzed the number of DNS verses TCP connections from unique IPs during the peak hour traffic that is collected from the sensors.

- *Classification technique 2* : **Hosts that use multiple DNS resolvers - Internal as well as External**
  - Hosts using organization's DNS servers as well as External DNS servers during the same time period.

What is Zeek?

Sniff traffic

~~IDS~~ NSM

Logs for various protocols seen in traffic

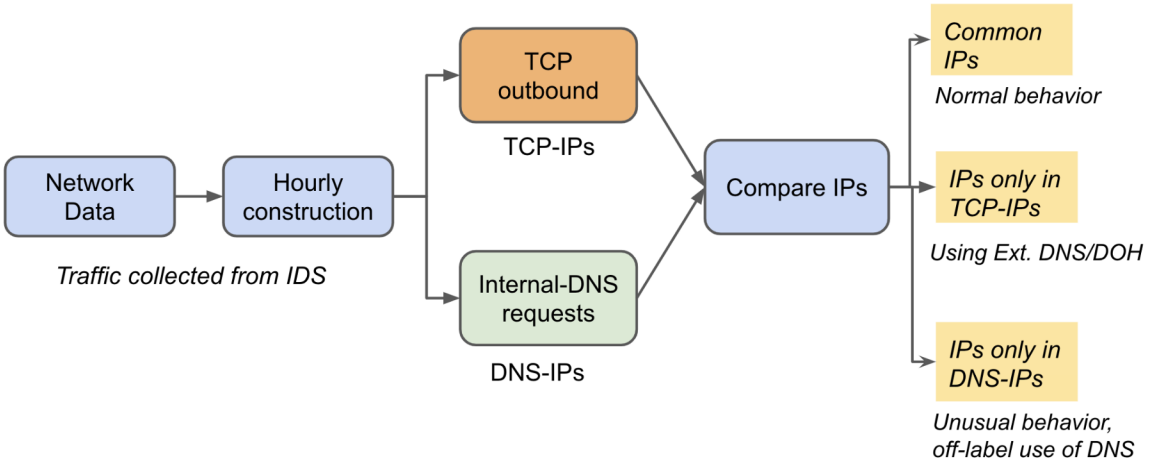
client_ip	latest_time	mac	dmacs	vendor	known_services	software_type	software_info
128.4	08/20/2017 15:01:33	10:41:7f	1	Apple, Inc.		iOS::IPHONE	iPhone,10,3,iPhone7,2AT&T
128.	08/20/2017 14:50:17	34:17:eb	1	Dell Inc.	22/tcp,(empty)	SSH::SERVER	OpenSSH,5,3,-
128.	08/20/2017 15:06:18.763725	78:2b:cb	1	Dell Inc.	22/tcp,SSH	SSH::SERVER	OpenSSH,6,6,p1
128.	08/20/2017 14:54:20	00:1e:68	1	QUANTA COMPUTER INC.	22/tcp,(empty)	SSH::SERVER	OpenSSH,5,9,p1
128.	08/20/2017 15:04:22.440988	90:b1:1c	1	Dell Inc.	22/tcp,SSH	SSH::SERVER	OpenSSH,6,6,-
128.	08/20/2017 14:51:21	14:da:e9	1	ASUSTek COMPUTER INC.	22/tcp,(empty)	SSH::SERVER	OpenSSH,7,2,p2
128.	08/20/2017 15:02:13	4c:cc:6a	1	Micro-Star INTL CO., LTD.	22/tcp,(empty)	SSH::SERVER	OpenSSH,7,2,p2
128.	08/20/2017 14:55:01	98:90:96	1	Dell Inc.		OS::WINDOWS	Windows,10,0,10
128.	08/20/2017 14:39:30	14:fe:b5	1	Dell Inc.		OS::WINDOWS	Windows,10,0,10
128.	08/20/2017 15:06:00.641491	e0:9d:31	1	Intel Corporate		OS::WINDOWS	Windows,6,1,7 or Server 2008 R2
128.	08/20/2017 15:06:21.108368	ac:87:a3:	1	Apple, Inc.		MACOS::MACINTOSH	Macintosh,10,10,Yosemite

Why use Zeek?

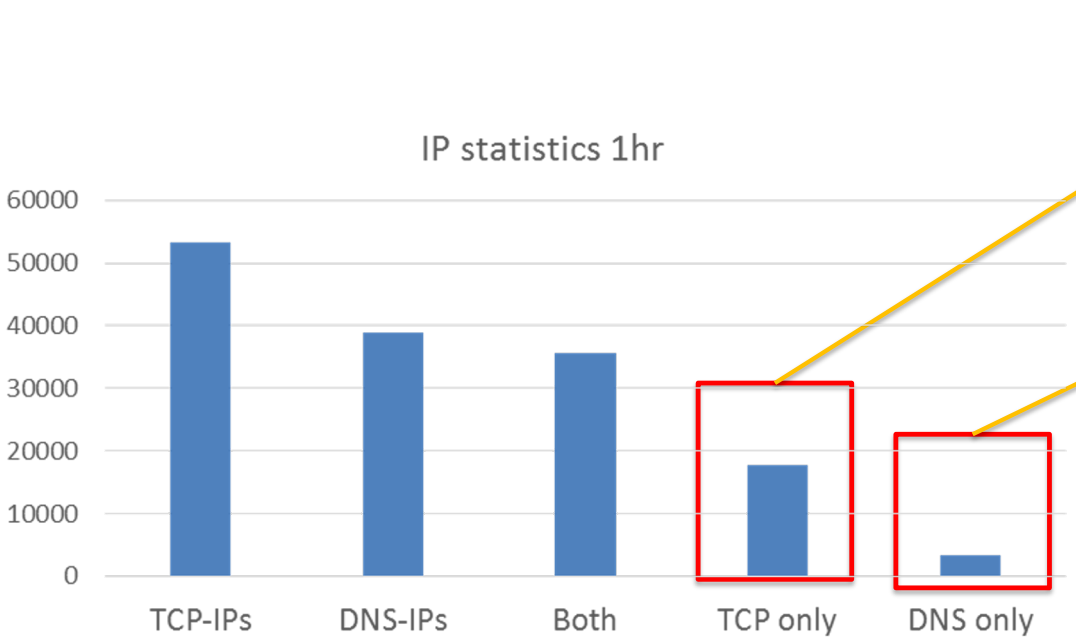
- It is a powerful network traffic analysis framework that is much different from the typical IDS you may know.
- One of the coolest features is, it's a great sniffer and generates [User-Friendly] logs of what it saw on the network. Take Advantage of that!
- Open Source free software with great community support.
- Holistic view of your network!

Classification technique 1
Hosts that never utilize DNS resolutions

- Proof of concept workflow for a sample time period (1hr) :
  - Find all unique IPs making TCP outbound connections
  - Find all unique IPs making DNS requests to Internal DNS servers – save as DNS-IPs



Results



Using External DNS/DOH

“off-label” use of DNS

Classification technique 1

Hosts that never utilize DNS resolutions

Case Study #1 : Hola VPN

- Hola VPN uses DNS probes to test the connectivity of the client to the internal DNS servers
- Detected more than 50 systems running Hola VPN by analyzing the DNS probes for domain “dns-test1.hola.org”. Out of which a dozen were used to send spam to the University clients
  - DNS probes for domain “zs-smtp-test.hola.org” were found corresponding to those hosts.

Case Study #1 : Hola VPN

Result - Used existing IT Governance procedures to remove and restrict use of Hola VPN on campus systems.

Case Study #1 : Hola VPN

IOCs that help detecting Hola VPN software:

Type of IOC	Value
Domain name	dns-test1.hola.org
Domain name	zs-smtp-test.hola.org
Domain name	http-test1.luminatinet.com
Domain name	zagent*.hola.org
HTTP user agent	Hola svc_js_*
HTTP Host	*.proxy_auth.trigger.hola.org

Classification technique 1

Hosts that never utilize DNS resolutions

Case Study #2: Antivirus software

McAfee: Uses DNS for Global Threat Intel (GTI) protection by providing access to an online cloud database containing file classification details to determine whether a file is malicious. (*.mvts.mcafee.com, *.mvqs.mcafee.com)

Case Study #2: Antivirus software

Sophos: Uses DNS for Sophos Extensible List to extend the protection by providing access to a wider amount of detection data/information when needed (*.sophosxl.net)

Case Study #2: Antivirus software - McAfee

- *How?*
  - GTI File Reputation looks for suspicious programs, Portable Document Format (PDF) files, and Android Application Package (.APK) files that are active on endpoints running McAfee products.
  - If any suspicious files are found that do not trigger existing signature DAT files, GTI sends a DNS request to a central database server hosted by McAfee Labs

Case Study #2: Antivirus software - McAfee

Information shared

GTI sends a fingerprint which includes Version and product information, File Hash, Fingerprint Information and Environmental Information.

McAfee DNS Query

Example query:

- 4z9p5tjmcbnblehp4557z1d136.avqs.mcafee.com or 4z9p5tjmcbnblehp4557z1d136.avts.mcafee.com

Case Study #2: Antivirus software - McAfee

McAfee DNS Response

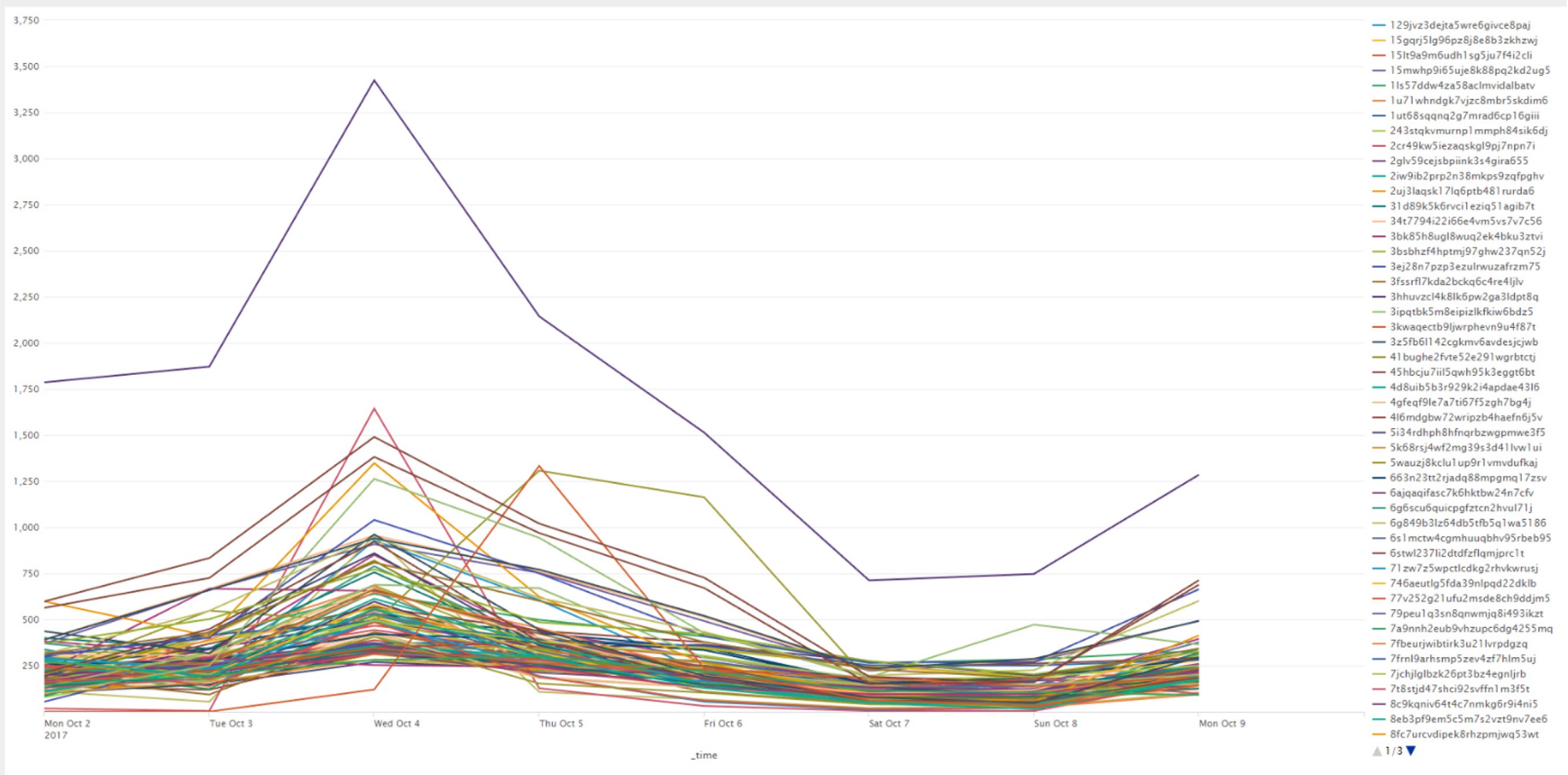
- *Two responses seen primarily from the McAfee for those DNS queries*

  NOERROR - hypothesis is when the queried file hash is found in the GTI DB

  NXDOMAIN - hypothesis is when the queried file hash is not found in the GTI DB

Case Study #2: Antivirus software - McAfee

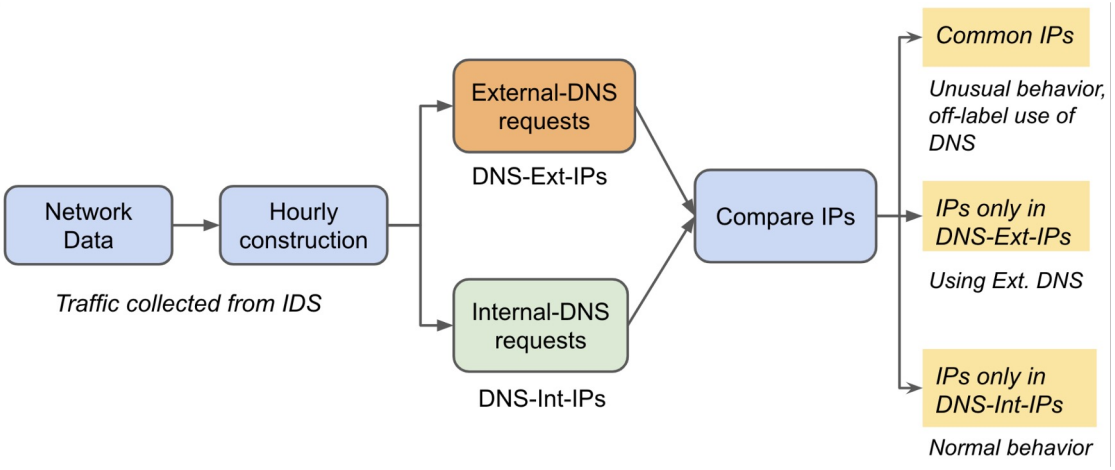
Result -Trending Malware/Suspicious files



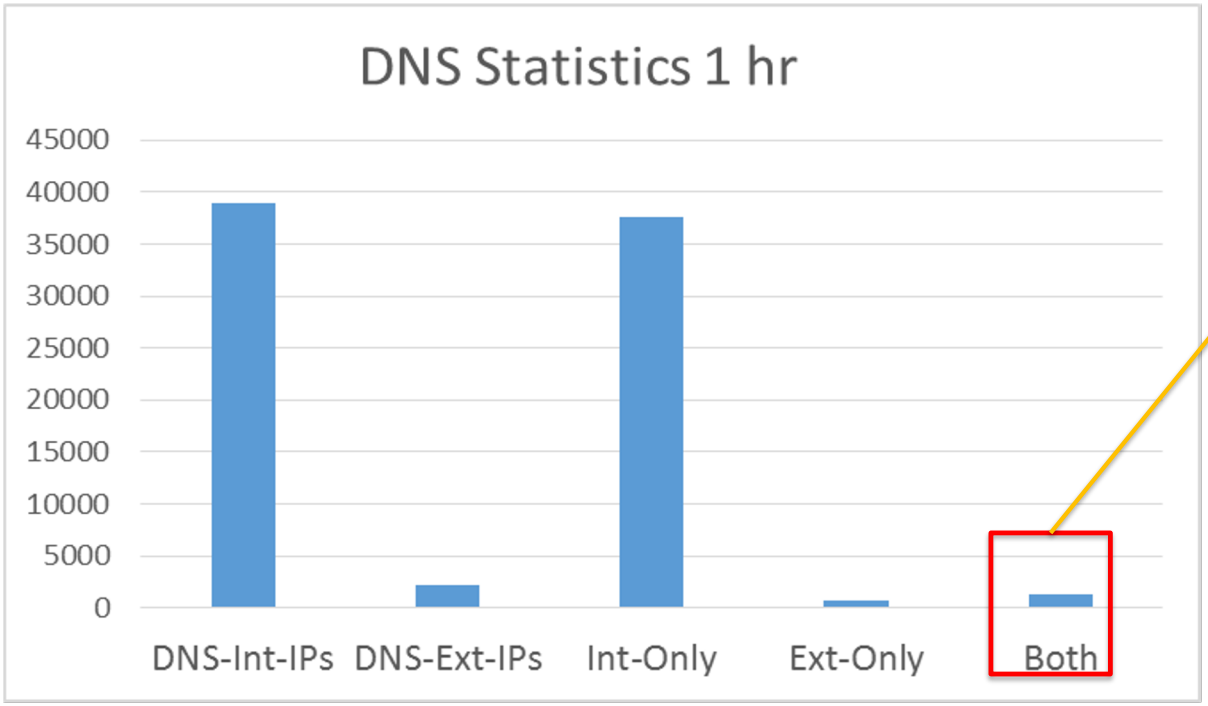
Classification technique 2:
Hosts using multiple DNS resolvers

Proof of concept workflow for a sample time period (1hr) :

- Find all unique IPs making DNS requests to Internal DNS servers – save as DNS-Int-IPs
- Find all unique IPs making DNS requests to External DNS servers – save as DNS-Ext-IPs



Results



Unusual Behavior, or "off-label" use of DNS?

Classification technique 2:
Hosts using multiple DNS resolvers

Case Study #3: Hosts running Balena OS

*"BalenaOS is an operating system optimized for running Docker containers on **embedded devices**, with an emphasis on reliability over long periods of operation, as well as a productive developer workflow."*

Case Study #3: Hosts running Balena OS

"DNSmasq manages the nameservers that NetworkManager provides for balenaOS. DNSmasq takes over and manage these nameservers to give the user the fastest most responsive DNS resolution."

Case Study #3: Hosts running Balena OS

- It's largely used for managing the fleets of embedded devices running Linux in core.
- If you run Balena Orchestration platform to manage your embedded (IoT like) devices, chances are they might be using the default configuration and might be *bypassing your DNS-RPZ or other DNS firewall !!*
- Result – Check for " api.balena-cloud.com" DNS queries in logs and reconfigure the systems to strictly use your organization's DNS servers.

Classification technique 2:
Hosts using multiple DNS resolvers

Case Study #4: Hosts running Avast Antivirus

- Some generic queries like following goes through Internal DNS servers:
  - emupdate.avast.com,
  - v7event.stats.avast.com,
  - uupdate.avast.com

Case Study #4: Hosts running Avast Antivirus

- More client specific queries goes to Google directly like following:
  - b3156325.iavs9x.u.avast.com
  - j3538725.iavs9x.avg.u.avcdn.net
- Provides “Real Site” protection for paid versions, provides an encrypted connection between your web browser and Avast's own DNS server to prevent DNS hijacking

Case Study #4: Hosts running Avast Antivirus

- Result-
  - Since every institution has some or other AV policies, and since many antivirus can be easily detected in the normal traffic, here's a script that detects major AV's:
    - https://github.com/fatemabw/bro-inventory-scripts/blob/master/scripts/AV_detection.bro
  - Detects McAfee, MalwareBytes, Avast, Sophos and Qihu

In conclusion…

- A lot of interesting things can be found out by analyzing DNS traffic
  - Malware is not the only application that misuses DNS, but legit applications as well!
  - We coined the term “off-label” use of DNS for the unconventional use of DNS by these legit applications

For complete paper:

“Off-Label” Use of DNS.
Fatema Bannat Wala and Chase Cotton. 2022.
ACM Digital Threats: Research And Practice Vol.3, (September 2022).
https://doi.org/10.1145/3491261

Thank You

Questions?